Journal of Trust Management
a SpringerOpen Journal

RESEARCH Open Access

Efficient private multi-party computations of trust in the presence of curious and malicious users

Shlomi Dolev[1*], Niv Gilboa[2] and Marina Kopeetsky[3*]

*Correspondence:
dolev@cs.bgu.ac.il;
marinako@sce.ac.il
[1]Department of Computer Science, Ben-Gurion University of the Negev, Beer-Sheva 84105, Israel
[3]Department of Software Engineering, Sami-Shamoon College of Engineering, Beer-Sheva 84100, Israel
Full list of author information is available at the end of the article

Abstract

Schemes for multi-party trust computation are presented. The schemes do not make use of a Trusted Authority. The schemes are more efficient than previous schemes in terms of the number of messages exchanged, which is proportional to the number of participants rather than to its square. We note that in our schemes the length of each message may be larger than the message length typically found in previously published schemes. The calculation of a trust, in a specific user by a group of community members starts following a request by an initiator. The trust computation is provided in a completely distributed manner, where each user calculates its trust value privately and independently. Given a community C and its members (users) $U_1, \ldots, U_n$, we present computationally secure schemes for trust computation. The first scheme, Accumulated Protocol *AP* computes the average trust attributed to a specific user, U_t following a trust evaluation request initiated by a user U_n. The exact trust values of each queried user are not disclosed to U_n. The next scheme, Weighted Accumulated Protocol *WAP* generates the average weighted trust in a specific user U_t taking into consideration the unrevealed trust that U_n has in each user participating in the trust evaluation process. The Public Key Encryption Protocol *PKEP* outputs a set of the exact trust values given by the users without linking the user that contributed a specific trust value to the trust this user contributed. The obtained vector of trust values assists in removing outliers. Given the set of trust values, the outliers that provide extremely low or high trust values can be removed from the trust evaluation process. We extend our schemes to the case when the initiator, U_n, can be compromised by the adversary, and we introduce the Multiple Private Keys and the Weighted protocols (*MPKP* and *MPWP*) for computing average unweighted and weighted trust, respectively. Moreover, the Commutative Encryption Based Protocol (*CEBP*) extends the *PKEBP* in this case. The computation of all our algorithms requires the transmission of $O(n)$ (possibly large) messages.

Keywords: Private trust computations; Multi-party computations; Anonymity

Our contribution

The purpose of this paper is to introduce new schemes for decentralized reputation systems. These schemes do not make use of a Trusted Authority to compute the trust in a particular user that is attributed by a community of users. Our objective is to compute trust while preserving user privacy.

We present new efficient schemes for calculating the trust in a specific user by a group of community members upon the request of an initiator. The trust computation is

provided in a completely distributed manner, where each user calculates its trust value privately. The user privacy is preserved in a computationally secure manner. The notions of privacy and privately computed trust, are determined in the sense that given an output average trust in a certain user, it is computationally infeasible to reveal the exact trust values in this user, given by community users. We assume a community of users $C = \{U_1, U_2, \ldots, U_n\}$. Let U_n be an initiator. The goal of U_n is to get an assessment of the trust in a certain user, U_t by a group consisting of $U_1, U_2, \ldots, U_{n-1}$ users from C. The *AP* calculates the average trust (or the sum of trust levels) in the user U_t (Section 'Accumulated protocol AP'). The *AP* protocol is based on a computationally secure homomorphic cryptosystem, e.g., the Paillier cryptosystem [1], which provides a homomorphic encryption of the secure trust levels $T_1, \ldots, T_{n-1}$ calculated by each user $U_1, U_2, \ldots, U_{n-1}$ from C. The *AP* satisfies the features of the Additive Reputation System [2] and does not take into consideration $U_n's$ subjective trust values in the queried users $U_1, U_2, \ldots, U_{n-1}$. A decentralized reputation system is defined as additive/non additive [2] if feedback collection, combination, and propagation are implemented in a decentralized way, and if a combination of feedbacks provided by agents is calculated in an additive/non additive manner, respectively. The *WAP* carries out a non additive trust computation (Section 'Weighted accumulated protocol WAP'). It outputs the weighted average trust which is based on the trust given by the initiator U_n in each C member participating in the feedback. The *WAP* is an enhanced version of the *AP* protocol. The *AP* and *WAP* protocols cope with a curious adversary and are restricted to the case of an uncompromised initiator, U_n. The *MPKP* and *MPWP* protocols, introduced in Section 'Multiple Private Keys Protocol *MPKP*', use additional communication to relax the condition that the initiator U_n is uncompromised and provide average unweighted and weighted privately computed trust, respectively.

Compared with the recent results in [2] and [3], our schemes have several advantages.

The Private Trust scheme is resistant against either curious or semi-malicious users The *AP* and *WAP* protocols preserve user privacy in a computationally secure manner. Our protocols cope with any number of curious but honest adversarial users. Moreover, the *PKEBP* (Section 'Protocols for removal of outliers') is resistant against semi-malicious users that return false trust values. The *PKEBP* supports the removal of outliers. The general case, when the initiator, U_n, can be compromised by the adversary, is addressed by the *MPKP*, *MPWP* and *CEBP* (Sections 'Protocols for removal of outliers' and 'Multiple Private Keys Protocol *MPKP*') protocols. Unlike our model, [2] suggests protocols that are resistant against curious agents who only try to collude in order to reveal private trust information. Moreover, the reputation computation in some of the algorithms in [3] contains a random parameter that reveals information about the reputation range of the queried users.

Low communicational overhead The proposed schemes require only $O(n)$ size messages to be sent, while the protocols of [2] and [3] require $O(n^3)$ communication messages.

No limitations on the number of curious users The computational security of the proposed schemes does not depend on the number of curious users in the community. Moreover, privacy is preserved regardless of the size of the coalition of curious users. Note that the number of the curious users should be no greater than half of the community users in the model presented in [2].

Background and literature review

The use of homomorphic cryptosystems in general Multiparty Computation (MPC) models is presented in [4]. In [4] it is demonstrated that, given keys for any sufficiently efficient homomorphic cryptosystem, general MPC protocols for n players can be devised such that they are secure against an active adversary who corrupts any minority group of the players. The problem stated and solved in [4] is as follows: given the encryptions of two numbers, say a and b (where each player knows only its input), compute securely an encryption of $c = ab$. The correctness of the result is verified. The total number of bits sent is $O(nkC)$, where k is a security parameter and C is the size of a Boolean circuit computing the function that should be securely evaluated. An earlier scheme proposed in [5] with the same complexity was only secure for passive adversaries. Earlier protocols had complexity that was at least quadratic in n. Threshold homomorphic encryption is used to achieve the linear communication complexity in [4]. The schemes proposed in [4,6], and [7] are based on public key infrastructure and use Zero Knowledge proofs (ZKP) as building blocks. When compared to [4,6], and [7] our schemes privately compute the average unweighted (additive) and weighted (non additive) characteristics, respectively, without using relatively hard-to-implement techniques such as ZKP.

Independently, (though slightly later than [8,9]), linear communication MPC was presented in [10]. A perfectly secure MPC protocol with linear communication complexity was proposed in [11]. Our model presented herein, (with a semi-honest but curious adversary) copes with at most $\frac{n}{2} - 1$ compromised users that supply arbitrary trust values, while [11] copes (in an information theoretic manner) with up to $\frac{n}{3}$ compromised users (even totally malicious users) with a similar communication overhead, $O(n^3 \cdot ln^3)$. Here, l denotes the total message length.

Following [8,9], privacy preserving protocols were investigated in [12] and [13]. Protocols for efficient multi-party sum computation (in the semi-honest adversarial model) are proposed in [12] and [13]. The derived protocols are augmented (by applying Zero Knowledge Proofs of plaintext equality and set membership) to handle malicious adversary. The simulation results demonstrate the efficiency of the designed methods. Compared with our results, the most powerful and efficient *StR* protocol of [12] and [13] is based on a completely connected network topology where each network user is directly connected to all other users. In addition, the schemes of [12] and [13] can be applied in the Additive Reputation Systems, while our schemes are designed also for the Non-Additive Reputation System.

Homomorphic ElGamal encryption is used in [6] as part of a scheme for multi-party private web search with untrusted partners (users). The scheme is based on multi-party computation that protects the privacy of the users with regards to the web search engine and any number of dishonest internal users. The number of sent messages is linear in the number of users (each of the n users sends $4n - 4$ messages). In order to obtain a secure permutation (of N elements), switches of the Optimized Arbitrary Size Benes network (OAS-Benes) are distributed among a group of n users, and the honest users control at least a large function $S(N)$ of the switches of the OAS-Benes. The proposed MPC protocol is based on the homomorphic threshold n-out of-n ElGamal encryption. Nevertheless, unlike our model, a MPC protocol is based on the computationally expensive honest-verifier ZKP protocol, and the Benez permutation network.

The efficient scheme for the secure two-party computation for "asymmetric settings" in which one of the devices (smart card, mobile device, etc.) is strictly computationally weaker than the other, is introduced in [7]. The workload for one of the parties is minimized in the presented scheme. The proposed protocol satisfies one-round complexity (i.e., a single message is sent in each direction assuming trusted setup).The proposed protocol performs only two-party secure computations, while the number of participants is not bounded in our schemes. Moreover, computationally expensive, Non Interactive Zero-Knowledge Proof techniques, and "extractable hash functions" are used in the scheme of [7].

A number of systematic approaches and corresponding architectures for creating reliable trust and reputation systems have been recently proposed in [14-18]. The main scope of these papers is the definitions of variety of settings for decentralized trust and reputation systems. A probabilistic approach for constructing computational models of trust and reputation, is presented in [17], where trust and reputation are studied in the scope of various social and scientific disciplines.

The computation models for the reputation systems of [16] support user anonymity by generating a pseudonym for any user, therefore, concealing user identity. In contrast to [16], the main challenge of our approach is to preserve the user anonymity in the computation process of the trust.

One of the common problems stated and discussed in [18] is that most existing reputation systems lack the ability to differentiate dishonest from honest feedback and, therefore, are vulnerable to malicious cooperations of users (peers in P2P systems) who provide dishonest feedback. The dishonest feedback is effectively filtered out in [18] by introducing the factor of feedback similarity between a user (pair) in the collusive group, and a user (peer) outside the group. We propose a different approach for the removal of dishonest users (outliers) by estimating the range of the correct trust values [19].

Two other works that are related to our scheme appear in [2] and [3]. In [2] several privacy and anonymity preserving protocols are suggested for an Additive Reputation System.

The authors state that supporting perfect privacy in decentralized reputation systems is impossible. Nevertheless, they present alternative probabilistic schemes for preserving privacy. A probabilistic "witness selection" method is proposed in [2] in order to reduce the risk of selecting dishonest witnesses. Two schemes are proposed. The first scheme is very efficient in terms of communication overhead, but this scheme is vulnerable to collusion of even two witnesses. The second scheme is more resistant toward curious users, but still is vulnerable to collusion. It is based on a secret splitting scheme. This scheme provides a secure protocol based on the verifiable secret sharing scheme [20] derived from Shamir's secret sharing scheme [21]. The number of dishonest users is heavily restricted and must be no more than $\frac{n}{2}$, where n is the number of contributing users. The communication overhead of this scheme is rather high and requires $O(n^3)$ messages.

An enhanced model for reputation computation that extends the results of [2] is introduced in [3]. The main enhancement of [2] is that a non additive (weighted) trust and reputation can be computed privately. Three algorithms for computing non additive reputation are proposed in [3]. The algorithms have various degrees of privacy and different levels of protection against adversarial users. These schemes are computationally secure regardless of the number of dishonest users.

The paper [22] (published later than [8,9]), proposes the distributed *Malicious-k-shares* protocol, which extends the results of [2] and [3] in the sense that a high majority of users (agents) can find k, $k << n$ sufficiently trustworthy agents in a set of $n - 1$ users-feedback providers. This protocol is based on homomorphic encryption and Non-Interactive Zero-Knowledge proofs. The *Malicious k-shares protocol* is applicable in the Additive Reputation System only, while our schemes privately compute also the weighted trust. The techniques, used for removal of outliers, is based on Non-Zero Knowledge Proofs of set-membership and plain-text equality, while the proof preserves that a certain share lies in the correct interval. The proposed protocol requires the exchange of $O(n + \log\ N)$ messages (where n and N are the number of users in the protocol and environment, respectively), while we use a more computationally effective techniques for removal of outliers exchanging only $O(n)$ messages.

We propose new efficient trust computation schemes that can replace any of the above schemes. Our schemes enable the initiator to compute unweighted (additive) and weighted (non additive) trust with low communication complexity of $O(n)$ (large) messages.

Table 1 summarizes the approaches proposed in this paper, computations that they perform, resistance to the different types of attacks and the crypto building blocks that are used.

This paper extends the schemes of [9] by introducing the *MPKP* and *MPWP* protocols that compute average unweighted and weighted trust in the general case, even when the initiator U_n can be compromised by the adversary. The proofs of correctness of the proposed protocols extend the presentations of [9] and [8].

Paper organization

The formal system description appears in Section 'Research design and methodology'. The computationally resistant (against curious but honest adversary) private trust protocol, *AP*, is introduced in Section 'Results and discussion' (Subsection "Accumulated protocol *AP*"). The enhanced version of *AP*, *WAP*, is presented in Section 'Results and discussion' (Subsection "Weighted accumulated protocol WAP"). The (resistant against semi-malicious users) *PKEBP* and *CEBP* and the scheme for removing outliers are presented in Section 'Results and discussion' (Subsection "Protocols for removal of outliers"). The generalized *MPKP* protocol and the weighted *MPWP* protocol are introduced in Section 'Results and discussion' (Subsection "Multiple Private Keys Protocol *MPKP*"). Conclusions appear in Section 'Conclusions'.

Research design and methodology

The purpose of this paper is to generate new schemes for private trust computation within a community. The contribution of our work is as follows: (a) the trust computation is

Table 1 Summary of the Presented Approaches

Protocol	*Computation*	*Adversarial model*	*Crypto building blocks*
AP	Average trust	Honest but curious	Homomorphic (of Paillier)
WAP	Weighted average trust	Honest but curious	Homomorphic (of Paillier)
PKEBP	Vector of exact trust; removal of outliers	Semi-malicious (restricted)	Any public key encryption
CEBP	Vector of exact trust; removal outliers	Semi-malicious (non restricted)	Commutative (Polhig-Hellman), ElGamal

performed in a completely distributed manner without involving a Trusted Authority. (b) the trust in a particular user within the community is computed privately. The privacy of trust values, held by the community users is preserved subject to standard cryptographic assumptions, when the adversary is computationally bounded. (c) The proposed protocols are resistant to a curious but honest poly-bounded k-listening adversary, Ad [23]. Such an adversary Ad may do the following: Ad may trace all the network links in the system and Ad may compromise up to k users, $k < n$. We require that an adversary Ad, compromising an intermediate node can only learn the node's trust values and an adversary Ad, compromising the initiator U_n can learn the output of the protocol, namely the average trust. We distinguish between two categories of adversaries: honest but curious adversaries, and semi-malicious adversaries [2]. An honest but curious k-listening adversary follows the protocol by providing correct input. Nevertheless, it might try to learn trust values in different ways, including collusion with, at most, k compromised users. While an honest but curious adversary does not try to modify the correct output of the protocol, a semi-malicious adversary may provide dishonest input in order to bias the average trust value.

Let $C = U_1, \ldots, U_n$ be a community of users such that each pair of users is connected via an authenticated channel. Assume that the purpose of a user U_n from C is to get the unweighted T_t^{avr} or weighted average trust wT_t^{avr} in a specific user, U_t, evaluated by the community of users. Denote by T^i, $i = 1 \,..\, n$, the trust of user U_i in U_t, and by $T_t^{avr} = \frac{\sum_{i=1}^{n} T^i}{n}$ and $wT_t^{avr} = 1/10 \sum_{i=1}^{n} w_i T^i$ the unweighted and weighted average trust in U_t, respectively. Here $w_i = 1, 2, \ldots, 10$ is the subjective trust of the initiator U_n in U_i in the form of an integer that facilitates our secure computation. In the subsequent work we always assume that w_i is an integer in this range. Denote by M_t the message sent by U_n to the first member of the community, C.

Our definitions of computational indistinguishability, simulation and private computation follow the definitions of [24]. Informally speaking, two probability ensembles are *computationally indistinguishable* if no polynomial time, probabilistic algorithm can decide with non-negligible probability if a given input is drawn from the first or the second ensemble. A distributed protocol computes a function f *privately* if an adversary cannot obtain any information on the input and output of other parties, beyond what is implicit in the adversary's own input and output. The way to prove that a protocol is private is to show that there exists a polynomial time, probabilistic *simulator* that receives as input the same input and output as an adversary and generates a string that is computationally indistinguishable from the whole view of the adversary, including every message that the adversary received in the protocol. Intuitively, the existence of a simulator implies that the adversary learns nothing from the execution of the protocol except its input and output.

Methods

The main tool we use in our schemes is public-key, homomorphic encryption. In such an encryption scheme there is a modulus, M, and an efficiently computable function ϕ that maps a pair of encrypted values $(E_K(x), E_K(y))$, where $0 \leq x, y < M$, to a single encrypted element $\phi(E_K(x), E_K(y)) = E_K(x+y \bmod M)$. In many homomorphic encryption systems the function ϕ is multiplication modulo some integer N. Given a natural number, c, and an encryption, $E_K(x)$, it is possible to compute $E_K(c \cdot x \bmod M)$, without knowing the

private key. Set $\beta = E_K(1)$ and let the binary representation of c be $c = c_k c_{k-1} \dots c_0$. Go over the bits $c_k, \dots, c_0$ in descending order. If $c_j = 0$, set $\beta = \phi(\beta, \beta)$ and if $c_j = 1$, set $\beta = \phi(\phi(\beta, \beta), E_K(x))$. If ϕ is modular multiplication, this algorithm is identical to standard modular exponentiation.

There are quite a few examples of homomorphic encryption schemes known in the cryptographic literature, including [1,25-28]. There are also systems that allow both addition and multiplication of two encrypted plaintexts, e.g., [29] where only a single multiplication is possible for a pair of ciphertexts, and [30]. All of these examples of homomorphic cryptosystems are currently assumed to be semantically secure [26].

Results and discussion

Accumulated protocol AP

The *AP* protocol may be based on any homomorphic encryption scheme such that the modulus N satisfies $N > \sum_{i=1}^{n} T_i$. We illustrate the protocol by using the semantically secure Paillier cryptosystem [1]. This cryptosystem possesses a homomorphic property and is based on the Decisional Composite Residuosity assumption. Let p and q be large prime numbers, and $N = pq$. Let g be some element of $Z^*_{N^2}$. Note that the base, g, should be chosen properly by checking whether $gcd(L(g^{\lambda} mod\ N^2), N) = 1$, where $\lambda = lcm(p-1, q-1)$, and the L function is defined as $L(u) = \frac{u-1}{N}$. The public key is the (N, g) pair, while the (p, q) pair is the secret private key. The ciphertext, c, for the plaintext message $m < N$ is generated by the sender as $c = g^m r^N \bmod N^2$, where $r < N$ is a randomly chosen number. The decryption is performed as $m = \frac{L(c^{\lambda} \bmod N^2)}{L(g^{\lambda} \bmod N^2)} \bmod N$ at the destination. Our schemes are based on the homomorphic property of the Paillier cryptosystem. Namely, the multiplication of two encrypted plaintexts m_1 and m_2 is decrypted as the sum $m_1 + m_2 \bmod N$ of the plaintexts. Thus, $E(m_1) \cdot E(m_2) \equiv E(m_1 + m_2 \bmod m) \bmod N^2$ and $E(m_1)^{m_2} \equiv E(m_1 \cdot m_2 \bmod N) \bmod N^2$. The *AP* protocol is described in Algorithm 1.

Algorithm 1 Accumulated Protocol.

1: *AP* **Initialization :**
2: U_n sets $A = 1$ and $M_t = A$
3: U_n sends M_t to U_1
4: *AP* **Execution :**
5: *for* $i = 1 \dots n-1$
6: $A = A \cdot E(T_i) \bmod N^2$
7: $M_t = A$
8: U_i sends M_t to U_{i+1}
9: *end for*
10: Upon M_t receipt at U_n
11: $S_t = D(M_t) = \sum_{i=1}^{n-1} T_i$
12: $T_t^{avr} = \frac{S_t}{n-1}$

Assume that the initiator, U_n, has generated a pair of its public and private keys as described above, and it has shared its public key with each community user. Then, U_n initializes to 1 the single entry trust message M_t and sends it to the first U_1 user (lines 1–3). Upon receiving the message, M_t, each node, U_i, encrypts its trust in U_t as $E(T_i) = g^{T_i} r_i^N \bmod N^2$. Here, T_i is a secret $U_i's$ trust level in U_t and r_i is a randomly generated

number. The $U_i's$ output is accumulated in the accumulated variable A multiplying its current value by the new encrypted $U_i - th$ trust $E(T_i)$ from the $i - th$ entry as $A = A \cdot (E(T_i))$. Then U_i sends the updated M_t message to the next user, U_{i+1}. This procedure is repeated until all trust values are accumulated in A (lines 4–9). The final M_t message received by the initiator, U_n is $M_t = A = \prod_{i=1}^{n} E(T_i) \bmod N^2$. As a result, the U_n user decrypts the value accumulated in the M message as the sum of trusts $S_t = D(M_t) = \sum_{i=1}^{n} T_i$. Thus, the average trust is $T_t^{avr} = \frac{S_t}{n-1}$ (Algorithm 1, lines 10–12). Proposition 1 proves that AP is a computationally private protocol to compute the trust of a community in U_t.

Proposition 1. Assume that an honest but curious adversary corrupts at most k users out of a community of n users, $k < n$. Then, AP privately computes T^{avr}, the average trust in user U_t.

Proof. In order to prove the proposition, we have to prove that for every adversary there exists a simulator that given only the adversary's input and output, generates a string that is computationally indistinguishable from the adversary's view in AP. Let $I = \{U_{i_1}, U_{i_2}, \ldots, U_{i_k}\}$ denote the set of users that the adversary controls. Let $view_I^{AP}(X_I, 1^n)$ denote the combined view of all users in I. $view_I^{AP}$ includes the input, $X_I = \{T_{i_1}, \ldots, T_{i_k}\}$, of all users in I, and a sequence of messages $E(\sum_{j=1}^{i_1} T_j), \ldots, E(\sum_{j=1}^{i_k} T_j)$ received by users in I. A simulator cannot generate the exact sequence $E(\sum_{j=1}^{i_1} T_j), \ldots, E(\sum_{j=1}^{i_k} T_j)$, since it does not have the input of uncorrupted users. Instead, the simulator chooses a random value α_j for any user $U_j \notin I$, from the distribution of trust values, D. The simulator denotes $\alpha_{i_1} = T_{i_1}, \ldots, \alpha_{i_k} = T_{i_k}$ and computes $E(\alpha_j)$ for $j = 1, \ldots, n-1$. The simulator now computes: $\prod_{j=1}^{i_1} E(\alpha_j) \equiv E(\sum_{j=1}^{i_1} \alpha_j) \bmod N^2, \ldots, \prod_{j=1}^{i_k} E(\alpha_j) \equiv E(\sum_{j=1}^{i_k} \alpha_j) \bmod N^2$. Hence, a simulator replaces $E(\sum_{j=1}^{i_k} T_j)$ by$E(\sum_{j=1}^{i_k} \alpha_j)$.

Assume, in contradiction, that there exists an algorithm DIS that distinguishes between the encryption of partial sums $E(\sum_{j=1}^{i_1} T_j), \cdots E(\sum_{j=1}^{i_k} T_j)$ of the correct trust values and the values $E(\sum_{j=1}^{i_1} \alpha_j), \cdots E(\sum_{j=1}^{i_k} \alpha_j)$ randomly produced by a simulator. We construct an algorithm, B, that distinguishes between the two sequences $E(T_1), \cdots E(T_{n-1})$ and $E(\alpha_1), \cdots, E(\alpha_k)$, contradicting the semantic security property of E. The input to algorithm B is a sequence of values $E(x_1), \cdots E(x_{n-1})$ and it attempts to determine whether the values $x_1, \ldots, x_{n-1}$ are equal to the values $T_1, \ldots, T_{n-1}$ that the users provide, or is a sequence of random values chosen from the distribution D. The algorithm B computes for every $\ell = 1, \ldots, k$

$$\prod_{j=1}^{i_\ell} E(x_j) \equiv E\left(\sum_{j=1}^{i_\ell} x_j\right) \bmod N^2,$$

and provides the encryption of partial sums $E(\sum_{j=1}^{i_1} x_j), \ldots E(\sum_{j=1}^{i_k} x_j)$ as input to DIS. B returns as output the same output as DIS. Since the input of DIS is $E(\sum_{j=1}^{i_1} T_j), \ldots E(\sum_{j=1}^{i_k} T_j)$ if and only if the input of B is $E(T_1), \ldots E(T_{n-1})$, we find that B distinguishes between its two possible input distributions with the same probability that DIS distinguishes between its input distributions. □

AP uses $O(n)$ messages each of length $O(n)$.

Weighted accumulated protocol WAP

The Weighted Accumulated *WAP* protocol, in addition to the *AP* protocol, generates the weighted average trust in a specific user, U_t, by the users in the community. The *WAP* protocol is based on an anonymous communications protocol proposed in [31] and on the homomorphic cryptosystem, e.g., Paillier cryptosystem [1]. It is described in Algorithm 2.

Algorithm 2 Weighted Accumulated Protocol *WAP*.

1: **WAP Initialization:**
2: U_n generates $TV = [E(w_1) .. E(w_{n-1})]$
3: U_n sets $A = 1$ and $M_t = (TV, A)$
4: **WAP execution:**
5: U_n sends M_t to U_1
6: *for* $i = 1 \ldots n-1$
7: $A = AE(w_i)^{T_i} E(\overline{0}) \bmod (N^2)$
8: Delete $TV[i]$
9: U_i sends M_t to U_{i+1}
10: *end for*
11: **Upon** M_t **reception at** U_n:
12: $S_t = D(A) = \sum_{i=1}^{n} w_i T_i$
13: $wT_t^{avr} = \frac{1}{10} \frac{S_t}{n-1}$

The initiator, U_n, generates $n-1$ weights $w_1, \ldots, w_{n-1}$. Each w_i value reflects the $U_n's$ subjective trust level in user U_i. U_n initializes the accumulated variable, A, to 1, encrypts each w_i value by means of, e.g., the Paillier cryptosystem [1] as $E(w_i) = g^{w_i} h^{r_{n,i}} (mod\ N^2)$, composes a Trust Vector $TV = [E(w_1) .. E(w_{n-1})]$ and sends the message $M_t = (TV, A)$ to U_1. Here, as in the *AP* case, p, q are large prime numbers which compose the Paillier cryptosystem, $N = (p-1)(q-1)$, and g and h are properly chosen parameters of the Paillier cryptosystem. $r_{n,i}$ is a random degree of h chosen by U_n for each U_i from C. Note that the *AP* protocol is a private case of the *WAP* protocol where all weights w_i are equal to 1.

As in the *AP* case, the M_t message is received by the community users in the prescribed order. Each U_i user encrypts its weighted trust in U_t as $E(T_i) = E(w_i)^{T_i} E(\overline{0})$ and accumulates it in the accumulated variable A (lines 6–10). Note that multiplying by the random encryption of zero $E(\overline{0})$ ensures semantic security of the *WAP* protocol since the user's output cannot be distinguished from a simulated random string. As a result, the initiator, U_n, receives the M_t message and decrypts the value accumulated in A as the weighted sum of trust $S_t = D(A) = \sum_{i=1}^{n-1} w_i T_i$. Therefore, the average trust is equal to $wT_t^{avr} = 1/10 \sum_{i=1}^{n} w_i T^i$. Proposition 2 proves the privacy of the weighted average trust wT_t^{avr} in the U_t user by the community users in a computationally secure manner.

Proposition 2. Assume that an honest but curious adversary corrupts at most k users out of a community of n users, $k < n$. Then, *WAP* privately computes wT^{avr}, the average weighted trust in user U_t.

Proof. The proof is similar to the proof of Proposition 1. View of adversary includes the input of compromised users $T_{i_1}, \ldots, T_{i_k}$, trust vector TV, and the accumulated variable, A. Each compromised user U_{i_j} from I receives $TV = [E(w_{i_j}),\ E(w_{i_{j+1}}) \ldots, E(w_n)]$ and $A = \prod_{i=1}^{i_j} E(w_i)^{T_i} E(\overline{0})$.

A simulator for the adversary simulates $view_I^{WAP}$ as follows. The simulator input $T_{i_1}, \ldots, T_{i_k}$ is the same as the input of the compromised users. A simulator chooses at random $\nu_1, \ldots, \nu_n$ according to a distribution, W, of weights, and $\widetilde{T_1}, \ldots, \widetilde{T_n}$ according to a distribution, D, of trust values. Here $\widetilde{T_{i_1}} = T_{i_1}, \ldots, \widetilde{T_{i_k}} = T_{i_k}$. Due to the semantic security of the homomorphic cryptosystem, the encrypted random values $E(\nu_1), \ldots, E(\nu_n)$ are indistinguishable from the encrypted correct weights $E(w_{i_1}), \ldots, E(w_{i_n})$.

The randomization of any $U_i - th$ user output is performed by multiplying its secret $w_i^{T_i}$ by the random encryption of a zero string $E(\overline{0})$. Given $E(w)$, the two values $E(w)^T$ and $E(u)$, where u is chosen at random from the distribution of wT, can be distinguished since T is chosen from a small domain of trust values. Given $E(w)$, the values $E(w)^T E(\overline{0})$ are distributed identically to an encryption $E(w)^T = E(wT \bmod N)$. Based on the semantic security of the homomorphic cryptosystem, $E(u)$ and $E(wT)$ cannot be distinguished even given $E(w)$. □

WAP uses $O(n)$ messages each of length $O(n)$.

Protocols for removal of outliers

The protocols for outliers removal are introduced in this section. The Public Key Encryption Based Protocol *PKEBP* produces a vector of the exact trust values. As a result, the initiator, U_n, can evaluate the correct trust range by removing the outliers that provide extremely high or low trust feedback. *PKEBP* preserves user privacy in a case where the adversary cannot corrupt the initiator and several users at the same time.

The generalized Commutative Encryption Based Protocol (*CEBP*) relaxes this limitation and privately computes the exact trust values contributed by each community user, even in the case when an adversary can corrupt the initiator and several users at the same time.

Public Key Encryption Based Protocol PKEBP

Denote the encryption algorithm used in this scheme by E and the decryption algorithm by D. U_n generates a pair (k, s) of public-private keys. Then U_n publishes its decryption public key k, while the private decryption key s is kept secret.

The Public Key Encryption Based Protocol *PKEBP* is performed in two rounds (Algorithm 3, Figure 1). At the initialization stage U_n initializes the $n-1$-entry vector $TV[1 \,..\, n-1]$ and sends it to the community of users in the prescribed order in the $M_t = (TV[1 \,..\, n-1])$ message (Algorithm 3, lines 1–2 and Figure 1, Round 1).

Algorithm 3 Vector Protocol *PKEBP*.

1: **Initialization:**
2: U_n initializes $TV =! [1 \,..\, n-1]$
3: **Round 1:**
4: U_n sends $M_t = TV[1 \,..\, n-1]$ to C
5: FOR $i = 1 \ldots (n-1)$
6: $TV[i] = E(T_i)$
7: END FOR
8: **Round 2:**
9: FOR $i = 1 \ldots (n-1)$
10: *random* π : $swap(TV[i], TV[i_j])$
11: END FOR
12: **Upon** $M_t = (TV[1 \,..\, n-1])$ **reception at** U_n**:**
13: $D(M) = [T_1, .. \, T_{n-1}]$

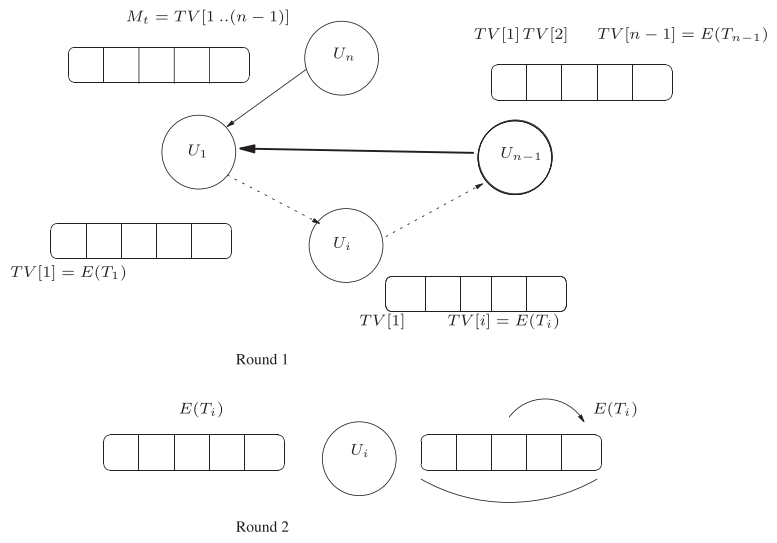

Figure 1 Public Key Encryption Based Protocol *PKEBP*.

In the first round, on reception of M_t each user, U_i, encrypts its trust, T_i, by k in the corresponding $TV[i]'s$ entry as $E(T_i)$, and sends the updated message M_t to the next user (Algorithm 3, lines 3–7).

The second round of the *PKEBP* protocol is performed when the updated $TV[1 .. n-1]$ vector returns from U_{n-1} to the user U_1 (see Algorithm 3, lines 8–11 and Figure 1, Round 2). Note that the TV vector does not visit the initiator U_n after execution of the first round. Each user, U_i, performs a random permutation of its $i-th$ entry with a randomly chosen $i_j - th$ entry during the second round. After that, the newly updated M_t vector-message is sent to the next U_{i+1} user (Algorithm 3, lines 8–11).

The result of round 1 is a sequence of encrypted elements $(E(T_1), \ldots, E(T_{n-1}))$ while the result of round 2 is a sequence $TV[1 .. n-1] = (E(T_1^*), \ldots, E(T_{n-1}^*))$. The multi-set $T_1, \ldots, T_{n-1}$ is identical to the multi-set $T_1^*, \ldots, T_{n-1}^*$. The sequence $T_1, \ldots, T_{n-1}$ is permuted to $T_1^*, \ldots, T_{n-1}^*$ by a permutation π, which is computed in a distributed manner by all community members (Algorithm 3, line 10). Thus, by applying the decryption procedure, all encrypted trust values $T_1, \ldots, T_{n-1}$ are revealed (Algorithm 3, lines 12–13). Moreover, the random permutation π performed at the second round preserves the unlinkability of user identities.

Proposition 3 proves the privacy of the *PKEBP* protocol.

Proposition 3. *PKEBP* performs computationally secure computation of exact private trust values assuming that an adversary cannot corrupt the initiator and several users at the same time.

Proof sketch. Case 1: $U_n \notin I$. We argue that *PKEBP* is private by showing that an adversary that controls a set of compromised users does not learn any information on the trust values of other users. We achieve that by showing a *simulator* that, given the input of compromised users, can simulate the messages that these users receive as part of the protocol. Therefore, protocol messages do not give users in I any information

on users outside of I. Assume that the set I of compromised users includes k members $I = \{U_{i_1}, \ldots, U_{i_k}\}$, while the uncompromised users are $U_{i_{k+1}}, \ldots, U_{i_n}$. The view of users in I includes the input of compromised users $T_{i_1}, \ldots, T_{i_k}$ and trust vectors TV. Each compromised user U_{i_j} from I receives the TV vector with partially permuted entries.

A simulator for the adversary simulates this view as follows. The simulator input is the same as the input of compromised users and it contains the trust values of the compromised users $T_{i_1}, \ldots, T_{i_k}$ and the set of their permuted indexes $i_j1, \ldots i_jk$. The simulator chooses a random value, α_{i_ℓ}, for any user $U_\ell \notin I$ from the distribution D of trust values. The simulator sets $\alpha_\ell = T_\ell$ and computes $E(\alpha_j)$ for $\ell = k+1, \ldots, n$. Due to the semantic security of the homomorphic cryptosystem [24,32], the simulator cannot distinguish between the encryption of the correct trust values and the encryption of simulated random variables, $E(\alpha_j)$, of uncompromised users, U_j, chosen from the distribution, D, of trust values.

Case 2: $\{U_n\} = I$. In this case, the view of U_n consists of the TV with the randomly permuted entries. TV includes the sequence of the randomly permuted exact trust values, decrypted by the secret key, s. We prove the privacy of *PKEBP* by showing a simulator that, given a *PKEBP* output sequence $T_{i_1}, \ldots, T_{i_{n-1}}$ of the exact trust values, can simulate the TV as U_n receives it as a part of the protocol. A simulator for the compromised U_n simulates this view as follows. The simulator input is the multi-set $T_1, \ldots, T_n$ of the exact trust values that have been decrypted by $U_n's$ public key, s. The simulator chooses a random permutation and permutes the received values. Due to the random permutation, π, performed by each community user, the simulator cannot distinguish between the simulated sequence $T_j1, \ldots, T_{j_{n-1}}$ and the correct output of the *PKEBP*.

As a result, given a multi-set of the exact trust values, U_n cannot link these values to the users that contributed them. □

PKEBP uses $O(n)$ messages each of length $O(n)$.

Generating the average trust level in the presence of semi-malicious users is based on the algorithm suggested in [19]. Let us define by U, the multi-set of non corrupted users which provide correct feedback, and by V, the multi-set of all users participating in the trust computation process. According to [19] the following requirement must be satisfied in our model: $|V - U| \leq J$ and $|V| \geq 2J$ for a certain J value. Then the range of the correct trust values, $range(U)$, contains the subset $reduce^J(V)$ of V. Here $reduce^J(V)$ is received from the V multi-set of all (correct and extremely low/high) trust values, by deleting the J smallest and J largest values, respectively.

If an adversary can corrupt the initiator and several users at the same time, a different protocol is required. The generalized Commutative Encryption Based Protocol *CEBP* is presented in the next subsection.

Commutative Encryption Based Protocol CEBP

The *CEBP* we propose, uses *commutative encryption* as a building block. An encryption scheme is commutative if a ciphertext that is encrypted by several keys can be decrypted regardless of the order of decryption keys. Formally, denote the encryption algorithm by E and the decryption algorithm by D. The encryption scheme is commutative if for every plaintext message m and every two keys k_1, k_2 if $c = E_{k_1}(E_{k_2}(m))$

then $m = D_{k_1}(D_{k_2}(c))$ (note that for any encryption scheme $m = D_{k_2}(D_{k_1}(c))$. One possible candidate for a commutative encryption scheme is the Pohlig-Hellman scheme [33].

The basic idea of *CEBP* is for each user to encrypt all the trust values and then decrypt and permute them at the same time so that an adversary cannot associate decrypted trust values with the users that published their encryption. The *CEBP* protocol is executed in three rounds (Algorithm 4). Each round passes sequentially from the first user U_n to the last U_{n-1}.

Algorithm 4 Commutative Encryption Based Protocol *CEBP*.

Round 1:
U_n chooses parameters for El-Gamal encryption p, q, g, k_n.
U_n initializes an empty vector $TV[1, \ldots, n-1]$.
U_n sends $p, q, g, g^{k_n} \bmod p$ and $TV[1, \ldots, n-1]$ to U_1.
FOR $i = 1, \ldots, n-1$
U_i chooses four Pohlig-Hellman key pairs $(a_i^1,\ b_i^1)$, $(a_i^2,\ b_i^2)$, (α_i^1, β_i^1), (α_i^2, β_i^2).
U_i sets $TV[i] = \left(g^{k_i a_i^1} \bmod p,\ (T_i g^{k_i k_n})^{\alpha_i^1} \bmod p\right)$.
U_i sends p, q, g, k_n and $TV[1, \ldots, n-1]$ to U_{i+1}.
END FOR
Round 2:
U_n sends $TV[1, \ldots, n-1]$ to U_1.
FOR $i = 1, \ldots, n-1$
FOR $j = 1, \ldots, n-1, j \neq i$
U_i sets $TV[j, 1] = (TV[j])^{\alpha_i^1 a_i^1} \bmod p$.
U_i sets $TV[j, 2] = (TV[j])^{\alpha_i^2 a_i^2} \bmod p$.
END FOR
U_i sets $TV[i, 1] = (TV[j])^{\alpha_i^1} \bmod p$.
U_i sets $TV[j, 2] = (TV[j])^{\alpha_i^2} \bmod p$.
U_i sends $TV[1, \ldots, n-1]$ to U_{i+1}.
END FOR
Round 3:
U_n sends $TV[1, \ldots, n-1]$ to U_1.
FOR $i = 1, \ldots, n-1$
FOR $j = 1, \ldots, n-1$
U_i sets $TV[j, 1] = (TV[j])^{\beta_i^1 b_i^1} \bmod p$.
U_i sets $TV[j, 2] = (TV[j])^{\beta_i^2 b \sum_i^2} \bmod p$.
U_i randomly permutes the $n-1$ elements of TV.
END FOR
U_i sends $TV[1, \ldots, n-1]$ to U_{i+1}.
END FOR
Epilogue:
U_n decrypts $TV[1, \ldots, n-1]$, thus obtaining the multi-set of trust values.

The first round begins with the initiator, U_n choosing and publishing a public key. Every other user selects a symmetric key for a commutative encryption scheme. All the users

encrypt their trust values both with their keys and with the public key of U_n. Encryption with the initiator's public key prevents an adversary that does not control the initiator, U_n, from obtaining the multi-set of trust values. After the first round, for every $i = 1, \ldots, n-1$, the i-th entry in the trust vector, TV, includes the trust value of U_i encrypted by both the public key of U_n and the symmetric key of U_i.

In the second round each user encrypts all entries in TV entries in such a way that at the end of the second round the i-th entry is the trust value of U_i encrypted by the keys of $U_1, U_2, \ldots, U_n$. Finally, in the third round, for every $i = 1, \ldots, n-1$, U_i decrypts every entry using its own symmetric key and randomly permutes the entries of TV. At the end of round 3 the trust vector contains all the trust values, encrypted by the public key of U_n and permuted. By decrypting all the entries in TV, U_n obtains the vector of all trust values.

We use El-Gamal encryption [34] as the initiator's public key scheme. The symmetric scheme for users $U_1, \ldots, U_{n-1}$ is Pohlig-Hellman. Both the Pohlig-Hellman and the El-Gamal schemes are implemented over the same group, which is defined as follows. Let p be a large prime, such that $p-1$ has a large prime factor, q. Let $g \in \mathbb{Z}_p^*$ be an element of order q in $\mathbb{Z}_p^*$. In a Pohlig-Hellman scheme, the key is a pair $a, b \in \mathbb{Z}_{p-1}^*$ such that $ab \equiv 1 \bmod (p-1)$. A plaintext $m \in \mathbb{Z}_p$ is encrypted by $c \equiv m^a \bmod p$ and a ciphertext is decrypted by $m \equiv c^b \bmod p$. In an El-Gamal scheme, the private key is $a \in \{0, \ldots, q-1\}$, the public key is $g^a \bmod p$ and a plaintext $m \in \mathbb{Z}_p$ is encrypted by the pair $(g^b \bmod p, g^{ab} \cdot m \bmod p)$. We refer to the two parts of an El-Gamal encryption as two *components*.

By using Pohlig-Hellman and El-Gamal encryption schemes over the same group we ensure that the security of *CEBP* can be reduced to the hardness of the Decisional Diffie-Hellman (DDH) problem [35]. The DDH problem is to distinguish between the two ensembles $\left(g^x \bmod p, g^y \bmod p, g^z \bmod p\right)$ and $\left(g^x \bmod p, g^y \bmod p, g^{xy} \bmod p\right)$. The hardness assumption of DDH is that no probabilistic, polynomial time algorithm can distinguish between these two probability ensembles with non-negligible probability.

The details of the protocol follow.

The initiator begins round 1 (lines 1–9) by choosing parameters for El-Gamal encryption and distributes its public key $g^{k_n} \bmod p$. Every other user U_i $(i = 1, \ldots, n-1)$ chooses four random and independent pairs of Pohlig-Hellman keys (a_i^1, b_i^1), (a_i^2, b_i^2), (α_i^1, β_i^1), (α_i^2, β_i^2). U_i uses the El-Gamal public key to encrypt its trust value, T_i. The result is $\left(g^{k_i} \bmod p,\ T_i g^{k_i k_n} \bmod p\right)$, where U_i chooses k_i randomly in the range $0, \ldots, q-1$. U_i proceeds to encrypt the El-Gamal encryption of T_i with its Pohlig-Hellman keys. Each of the two components of the El-Gamal encryption is encrypted by one distinct Pohlig-Hellman key. The result is

$$\left(g^{k_i a_i^1} \bmod p,\ (T_i g^{k_i k_n})^{a_i^2} \bmod p\right).$$

U_i completes the round by publishing this value in $TV[i]$. We think of $TV[i]$ as having two components, $TV[i,1]$ and $TV[i,2]$. U_i stores $g^{k_i a_i^1} \bmod p$ in $TV[i,1]$ and stores $(T_i g^{k_i k_n})^{a_i^2} \bmod p$ in $TV[i,2]$.

In round 2, every user, U_i, $i = 1, \ldots, n-1$ makes sure that every entry in $TV[]$ is encrypted with all four of its Pohlig-Hellman encryption keys (where two of the keys are

used to encrypt the left component and two are used to encrypt the right component). Thus, U_i encrypts $TV[i]$ with α_i^1 and α_i^2 and encrypts $TV[j]$ for any $j \neq i$ with a_i^1, a_i^2, α_i^1 and α_i^2. After the second round the entry $TV[i]$ holds the value:

$$\left(g^{k_i \cdot \alpha_1^1 a_1^1 \cdot \ldots \cdot \alpha_{n-1}^1 a_{n-1}^1} \bmod p,\ (T_i g^{k_i k_n})^{\alpha_1^2 a_1^2 \cdot \ldots \cdot \alpha_{n-1}^2 a_{n-1}^2} \bmod p\right).$$

In round 3, the users both decrypt and permute all the values. Each user decrypts all values using both its pairs of Pohlig-Hellman keys (lines 20–27) and then randomly permutes the resulting vector of values. Due to the commutative property of the scheme, the initiator, U_n, holds all the trust values at the end of round 3. However, the random permutation each user applies to the encrypted values in round 3 ensures that even if only a pair of users is not compromised, the decrypted trust values are randomly permuted in relation to their associated users.

Proposition 4. Assume that the DDH problem is hard and assume that an honest but curious adversary corrupts at most k users out of a community of n users, $k \leq n$. If the trust values of all the users are in the sub-group generated by g, then, *CEBP* privately computes the set of all trust values of community users.

Proof sketch. If the adversary controls at least $n-1$ users, including the initiator, then the protocol is trivially private, since the output reveals the exact trust values of every user, and thus any protocol does not add information. If the adversary does not control the initiator then the protocol is private because all trust values are encrypted by the initiator's public key throughout the protocol. Since the El-Gamal encryption scheme is semantically secure, given the hardness of DDH problem, it is easy to argue privacy.

Therefore, the most interesting case is when $k \leq n-2$ and the adversary controls the initiator. To prove privacy we define a simulator that is given the adversary's input and output (which includes the set of trust values) and simulates the adversary's view of protocol messages.

Each message in our protocol consists of the trust vector TV. Each entry in this vector is a pair of elements in $\mathbb{Z}_p^*$. Thus, the whole view of the adversary can be written as $e_1, \ldots, e_m$, where $e_i \in \mathbb{Z}_p^*$ for every $i = 1, \ldots, m$. The value of m is at most $O(n^2)$ because the number of elements in TV is $2(n-1)$ and the adversary receives a message with TV in it at most $n-2$ times for each of the three rounds.

Note that each element e_i is obtained by raising g to a power η_i that depends on the input and random coin tosses of each participant. The simulator generates a simulated view $f_1, \ldots, f_m$ as follows. If η_i is determined by the input and coin tosses of the adversary, then the simulator who has access to this input and coin tosses sets $f_i = e_i$. However, if η_i is generated at least partially by an uncorrupted node then the simulator independently chooses a random element $\zeta_i \in \{0, \ldots, q-1\}$ and sets $f_i = g^{\zeta_i}$.

To prove that the simulator's view is computationally indistinguishable from the real-world view, we construct a series of hybrid ensembles $H_0, \ldots, H_m$, such that H_0 is the real world view $e_1, \ldots, e_m$ and for every $i = 1, \ldots, m$ we define $H_i \stackrel{\triangle}{=} f_1, \ldots, f_i, e_{i+1}, \ldots, f_m$. Essentially, H_m is the view of the simulator.

We can show that for every i, if H_i can be computationally distinguished from H_{i+1} then the DDH assumption is false. Since we assume that DDH is a hard problem we have that

H_i and H_{i+1} are computationally indistinguishable and since m is of polynomial size in n, we have that H_0 is indistinguishable from H_m, completing the proof. □

The protocol requires $O(n)$ messages, each of length $O(n)$ and the computation complexity for each participant in the scheme is $O(n)$.

Multiple Private Keys Protocol *MPKP*

The *AP* and *WAP* protocols introduced in the previous sections carry out private trust computation assuming that the initiator U_n is not compromised and does not share its private key with other users. In the rest of this work assume that any community user, including U_n, may be compromised by a poly-bounded k-listening curious adversary.

The generalized Multiple Private Keys Protocol *MPKP* copes with this problem and outputs the average trust. The idea of the *MPKP* protocol is as follows. During the initialization stage the U_n user initializes all entries of trust vector, *TV*, and accumulated vector, *AV*, to 1, sets the accumulated variable A to 1, and sends the $M_t = (TV, AV, A)$ message to the first community user U_1 as in the previous protocols. During the first round of the *MPKP* protocol execution each user, U_i, randomly fragments its secret trust, T_i, to a sum of $n-1$ shares, encrypts the corresponding share by the public key of each U_j, $j = 1 \,..\, n-1$ user and accumulates its encrypted shares (multiplying each of them with the corresponding entries) in the accumulated vector, *AV*. After execution of the first round, the updated *AV* vector does not return to the initiator U_n. The *AV* vector visits each community user, while each U_i opens the $i-th$ entry (that is encrypted by $U_i - th$ public key) revealing a sum of decrypted shares, encrypts this sum by the public key of the initiator U_n, accumulates this sum in the accumulated variable ,A, and deletes the $i-th$ entry of the *AV* vector.

A detailed description of the *MPKP* protocol follows. Assume that each community user, U_i, $i = 1 \,..\, n-1$ generates its personal pair (P_i^+, P_i^-) of private and public keys. Denote by E_i and D_i the encryption and decryption algorithms produced by U_i. The private key, P_i^+, is kept secret, while the public key, P_i^-, is shared with all other users $U_1, \ldots, U_{i-1}, U_{i+1} \ldots U_n$. As in the previous schemes, the cryptosystem must be homomorphic. An additional requirement is that the homomorphism modulus, m, must be identical for all users. One possibility is to use the Benaloh cryptosystem [28,36] for which many different key pairs are possible for every homomorphism modulus. The system works as follows. Select two large primes, p, q, such that: $N \stackrel{\triangle}{=} pq$, $m|p-1$, $\gcd(m, (p-1)/m) = 1$ and $\gcd(m, q-1) = 1$, which implies that m is odd. The density of such primes along appropriate arithmetic sequences is large enough to ensure efficient generation of multiple p, q (see [36] for details). Select $y \in \mathbb{Z}_N^*$ such that $y^{\phi(N)/m} \not\equiv 1 \bmod N$. The public key is (N, y), and encryption of $M \in \mathbb{Z}_m$ is performed by choosing a random $u \in \mathbb{Z}_m^*$ and sending $y^M u^m \bmod N$. In order to decrypt, the holder of the secret key computes at a preprocessing stage $T_M \stackrel{\triangle}{=} y^{M\phi(N)/m} \bmod N$ for every $M \in \mathbb{Z}_m$. It should be noted that m is small enough such that m exponentiations can be performed. Decryption of z is performed by computing $z^{\phi(N)/n} \bmod N$ and finding the unique T_M to which it is equal.

The *MPKP* is performed in two rounds (Algorithm 5). The initialization procedure is shown in lines 1–4. The first round is the accumulation round, where all users share

their secret trust T_i values with other users. Upon reception of a message, M_t, each user, U_i, proceeds as follows: (a) U_i chooses $r_1^i, \ldots, r_{n-1}^i$ uniformly at random such that $T_i = \sum_{j=1}^{n-1} r_j^i$; (b) U_i encrypts each r_j^i, $j = 1 \,..\, n-1$ by the public key P_j^- of the U_j user and multiplies it by the current value stored in $j-th$ entry of AV. As a result, the output AV vector contains the accumulated product $\prod_{k=1}^{n-1} E_j(r_j^k)$ in each $j-th$ entry (lines 5–12).

Algorithm 5 Multiple Private Keys Protocol MPKP.

1: **MPKP Initialization:**
2: U_n generates $TV = [1 \,..\, 1]$
3: U_n sets $AV = [1 \,..\, 1]$, $A = 1$ and $M_t = (TV, AV, A)$
4: U_n sends M_t to U_1
5: **Round 1:**
6: *for* $i = 1 \ldots (n-1)$
7: $T_i = \sum_{j=1}^{n-1} r_j^i$
8: *for* $j = 1 \ldots (n-1)$
9: $AV[j] = AV[j]\, E_j(r_j^i)$
10: *end for*
11: U_i sends M_t to U_{i+1}
12: *end for*
13: **Round 2:**
14: *for* $i = 1 \ldots (n-1)$
15: $D_i(AV[i]) = \sum_{j=1}^{n-1} r_i^j$
16: $A = AE_n(\sum_{j=1}^{n-1} r_i^j)$
17: Delete $AV[i]$
18: *end for*
19: **Upon** $M_t = (A)$ **reception at** U_n**:**
20: $A = \prod_{i=1}^{n-1} E_n(\sum_{j=1}^{n-1} r_i^j)$
21: $S_t = D_n(A)$
22: $T_t^{avr} = \frac{S_t}{n-1}$

In the second round, on reception of message M_t, each user, U_i, decrypts the M_t message and decrypts the corresponding $i-th$ entry by its private key, P_i^+, computes the $\sum_{j=1}^{n-1} r_i^j$ sum, encrypts it by the $U_n's$ public key, P_n^-, as $E_n(\sum_{j=1}^{n-1} r_i^j)$, accumulates this sum in the accumulated variable, A, deletes the $i-th$ entry and sends the updated TV vector to the next U_{i+1} user. Note that the partial sum $\sum_{j=1}^{n-1} r_i^j$ that U_i decrypts reveals no information about correct trust values. As a result of the second round the initiator U_n receives $A = \prod_{i=1}^{n-1} E_n(\sum_{j=1}^{n-1} r_i^j)$ (lines 13–19). U_n decrypts $\prod_{j=1}^{n-1} E_n(r_i^j)$, and computes the sum of trusts as $S_t = \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} r_i^j$. Actually, the average trust T^{avr} is equal to $\frac{S_t}{n}$ (lines 20–22). Proposition 4 states the privacy of the *MPKP* protocol. The communication complexity of the *MPKP* protocol is $O(n)$ messages, each of length $O(n)$.

Proposition 5. *MPKP* performs computationally secure computation of the exact private trust values in the Additive Reputation System. No restriction is imposed on the initiator U_n.

The last introduced protocol is the *MPWP* for the weighted average trust wT_t^{avr} computation. The idea of the *MPWP* is as follows. During the initialization stage the U_n user generates a vector, TV, such that each $i-th$ entry contains the U_i-th weight w_i encrypted

by the $U_n - th$ public key. U_n sends TV and a $(n-1) \times (n-1)$ matrix, SM, with all entries initialized to 1 to the first community user, U_1, as in the previous protocols. During the first round of the *MPWP* execution each U_i computes its encrypted weight in the power of its secret trust $E_n(w_i)^{T_i}$, multiplies it by a randomly chosen number (bias) z_i, and accumulates the product in the accumulated entry (by multiplying the entry by the obtained result). In addition, U_i fragments its bias, z_i, into $n-1$ shares, encrypts each $j - th$ share by the public key of U_j, and inserts it in the $j - th$ location of $i - th$ matrix row. At the end of the first round U_n decrypts the total biased weighted trust. The total random bias is removed during the second round of the *MPWP* execution when each U_j decrypts the entries of $j - th$ matrix column, encrypts the sum of these values by the public key of the initiator, accumulates it in an accumulation variable, A, and deletes the $j - th$ column.

The details follow. The initiator, U_n, starts the first round by generating the encryption of the $n-1$ entries trust vector, $TV = [E_n(w_1) \,..\, E_n(w_{n-1})]$. Note, that each weight w_i is encrypted by the $U_n - th$ public key, P_n^-. In addition, U_n initializes to 1 each entry of the $(n-1) \times (n-1)$ matrix of shares SM. The M_t^w message sent by U_n to the community users is $M = (TV, SM)$. Upon the TV vector reception each U_i user proceeds as follows: (a) U_i computes $E_n(w_i)^{T_i} \cdot z_i$. Here z_i is a randomly generated by U_i number that provides the secret bias. (b) U_i accumulates its encrypted weighted trust in the accumulated variable A by setting $A = A \cdot E_n(w_i)^{T_i} \cdot z_i$. After that, the $i - th$ entry of TV is deleted. (c) U_i shares z_i in the $i - th$ row of the SM shares matrix as $SM[i][] = [E_1(z_i^1) \,..\, E_{n-1}(z_i^{n-1})]$. At the end of the first round U_n receives the $TV[]$ entry that is equal to the biased product $BT = \prod_{j=1}^{n} E_n(w_i)^{T_i} z_i$, encrypted by its public key, and the updated shares matrix SM while $SM[i][j] = E_j(z_i^j)$. Actually, the decryption procedure applied on the $TV[\,]$ vector outputs the decrypted sum $D(TV[]) = \sum_{i=1}^{n-1} w_i T_i + \sum_{i=1}^{n-1} z_i$. A second round is performed in order to subtract the random bias $\sum_{i=1}^{n-1} z_i$ from the correct weighted average trust wT^{avr}. The second round of the *MPWP* is identical to the corresponding round of the *MPKP*. Upon reception of the SM matrix each user, U_i, decrypts the corresponding $i - th$ column $E_i(z_1^i)\ E_i(z_2^i) \ldots E_i(z_{n-1}^i)$, encrypted by all community users by $U_i - th$ public key, P_i^-. Each $U_i,\ i = 1 \,..\, n-1$ computes the sum of the partial shares $PSS_i = \sum_{j=1}^{n-1} z_j^i$, encrypts it by the $U_n - th$ public key, P_n^-, and accumulates it in the accumulated variable A. After that, $i - th\ SM's$ column $SM[][i]$ is deleted. As a result of the second round, the initiator, U_n, receives the accumulated variable, $A = \prod_{i=1}^{n-1} E_i(PSS_i)$. The encrypted bias, BT, is decrypted as $D(A) = \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} z_j^i$.

Finally, the weighted average trust wT^{avr} is equal to $wT^{avr} = TV - A$. The private trust computation carried out by the *MPKP* and the *MPWP* protocols is preserved in the computationally secure manner due to the following reasons:

(a) Each community user, U_i, fragments its trust, T_i, randomly into $n-1$ shares (Algorithm 5, lines 6–8).

(b) Each r_i^j encrypted by U_i by the $U_j - th$ public key, P_j^-, shared with each $U_j, j = 1, \ldots, n-1$ user and accumulated in the TV vector, reveals no information about the exact T_i value to U_j (lines 9–14).

(c) The decryption performed by each $U_i, i = 1, \ldots, n-1$ by its private key, P_i^+, at the second round, outputs the sum of the partial shares, $D_i(TV[i]) = \sum_{j=1}^{n-1} r_j^i$ of all community users. In essence, the $\sum_{j=1}^{n-1} r_j^i$ value reveals no information about the secret trust values $T_1, \ldots, T_{i-1},\ T_{i+1}, \ldots, T_{n-1}$.

(d) The encryption $E_n(\sum_{j=1}^{n-1} r_j^i)$ of the partial shares sum performed by each U_i with the initiator U_n public key P_n^- and accumulated in A, can be decrypted by U_n only.

(e) Assume a coalition $U_{j_i}, \ldots, U_{j_{i+k-1}}$ of at most $k < n$ curious adversarial users, possibly including the initiator U_n. Then the exact trust values revealed by the coalition, are the coalition members trust only. The privacy of the uncorrupted users is preserved by the homomorphic encryption scheme which generates for each user its secret private key, and by the random fragmentation of the secret trust.

In *MPWP*, $O(n)$ messages of length $O(n^2)$ are sent.

Conclusions

We derived a number of schemes for the private computation of trust in a given user by a community of users. Trust computation is performed in a fully distributed manner without involving a Trusted Authority. The proposed *AP* and *WAP* protocols are computationally secure, under the assumption of an uncompromised initiator, U_n. The *AP* and *WAP* protocols compute the average unweighted and weighted trust, respectively. The generalized *MPKP* and *MPWP* protocols relax the assumption that U_n is non-compromised. They carry out the private unweighted and weighted trust computation, respectively, without limitations imposed on U_n. The number of messages sent in the proposed protocols is $O(n)$ (large) messages.

The *PKEBP* and *CEBP* for the removal of outliers are presented as well.The protocols, introduced and analyzed in this paper, may be efficiently applied in the fully distributed environment without any trusted authority. Compared with other models, our schemes privately compute trust values with low communication overhead of $O(n)$ (large) messages in the simplified ring network topology. The schemes may be applied to complete topology systems when all network users are connected by direct links. The schemes may be attractive in the case when sending the linear number ($O(n)$) of large messages is better than sending a substantially larger number ($O(n^3)$) of possibly smaller messages. Moreover, the outliers removal (performed by the *CEBP* protocol) may be efficiently performed by the computationally restricted users when there are no resources for generating computationally expensive Interactive and Non Interactive Zero Knowledge Proofs. The schemes proposed in this paper are not restricted to trust computation. They may be extended to other models that compute privately sensitive information with only $O(n)$ messages.

In a case where the trust is represented by several values rather then a single value, one can apply our techniques to each such value independently.

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
All authors read and approved the final manuscript.

Acknowledgments
Supported by Deutsche Telekom Laboratories at Ben-Gurion University of the Negev, Israel, Rita Altura Trust Chair in Computer Sciences, ICT Programme of the European Union under contract number FP7-215270 (FRONTS), Lynne and William Frankel Center for Computer Sciences, and the internal research program of the Sami Shamoon College of Engineering. The paper is a full version of two extended abstracts each describing a different part of the results [8,9].

Author details
[1]Department of Computer Science, Ben-Gurion University of the Negev, Beer-Sheva 84105, Israel. [2]Department of Communication Systems Engineering, Ben-Gurion University of the Negev, Beer-Sheva 84105, Israel. [3]Department of Software Engineering, Sami-Shamoon College of Engineering, Beer-Sheva 84100, Israel.

Received: 27 May 2013 Accepted: 22 January 2014
Published: 9 June 2014

References

1. Paillier P (1999) Public-key cryptosystems based on composite degree residuosity classes. Advances in cryptology, EUROCRYPT 99. Springer Berlin Heidelberg, pp 223–238
2. Pavlov E, Rosenschein JS, Topol Z (2004) Supporting privacy in decentralized additive reputation systems. Trust Management, Springer Berlin Heidelberg, pp 108–119
3. Gudes E, Gal-Oz N (2009) A grubshtein: methods for computing trust and reputation while preserving privacy. Proceedings of 23rd Annual IFIP WG 11.3 Working Conference on Data and Applications Security, Springer Berlin Heidelberg, pp 291–298
4. Cramer R, Damgard IB, Buus Nielsen J (2001) Multiparty computation from threshold homomorphic encryption. In: EUROCRYPT '01: proceedings of the international conference on the theory and application of cryptographic techniques. Springer, Berlin Heidelberg, pp 280–299
5. Franklin M, Haber S (1996) Joint encryption and message-efficient secure computation. J Cryptology 9(4):217–232
6. Romero-Tris C, Castella-Roca J, Viejo A (2012) Multi-party private web search with untrusted partners. Security and Privacy in Communication Networks, Springer Berlin Heidelberg. pp. 261-280. In: Rajarajan M, et al., Proceedings of SecureComm 2011, pp 261–280
7. Damgard I, Faust S, Hazay C (2012) Secure two-party computation with low communication. In: Cramer R (ed) TCC 2012, LNCS 7194, pp 54–74
8. Dolev S, Gilboa N, Kopeetsky M (2010) Computing trust privately in the presence of curious and malicious users. In: Proceedings of the international symposium on stochastic models in reliability engineering, life sciences and operations management. Sami Shamoon College of Engineering, Beer-Sheva, Israel
9. Dolev S, Gilboa N, Kopeetsky M (2010) Computing multi-party trust privately in *O(n)* time units sending one (possibly large) message at a time. In: Proceedings of 25-th Symposium On Applied Computing (SAC 2010), Sierre, Switzerland, pp 1460-1465
10. Asharov G, Jain A, Tromer E, Vaikuntanathan N, Wichs D (2012) Multiparty computation with low communication, computation and interaction via threshold FHE In: Proceedings of the EUROCRYPT 2012, pp 483–501. 2012
11. Beerliova-Trubmiova Z, Hirt M (2008) Perfectly-secure mpc with linear communication complexity. TCC2008, LNCS 4948: 213–230
12. Dimitriou T, Michalas A (2012) Multi-party trust computation in decentralized environment. In: Proceedings of the 5-th, IFIP international conference on New Technologies, Mobility and Security (NTMS 2012), Istanbul, Turkey
13. Dimitriou T, Michalas A (2013) Multi-party trust computation in decentralized environments in the presence of malicious adversaries. Ad Hoc Netw J. Elsevier, http://dx.doi.org/10.1016/j.adhoc.2013.04.013
14. Bachrach Y, Parnes A, Procaccia AD, Rosenschein JS (2009) Gossip-based aggregation of trust in decentralized reputation systems. Autonomous Agents, Multi-Agent Syst 19(2):153–172
15. Huynh TD, Jennings NR, Shadbolt NR (2004) An integrated trust and reputation model for open multi-agent systems. In: Proceedings of 16th European Conference on Artificial Intelligence, Spain, pp 18-22
16. Kinateder M, Rothermel K (2003) Architecture and algorithms for a distributed reputation system. Trust, Management, Vol. 2692, pp 1-16. Springer Berlin Heidelberg
17. Mui L, Mohtashemi M, Halberstadt A (2002) A computational model of trust and reputation. System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on. IEEE/pp 1435–1439
18. Xiong L, Liu L (2004) PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. IEEE Trans. Knowl Data, Eng 16(7):843–857
19. Dolev D, Lynch NA, Pinter SS, Stark EW, Weihl WE (1986) Reaching approximate agreement in the presence of faults. J ACM 33(3):499–516
20. Pedersen TP (1991) Non-interactive and information theoretic secure verifiable secret sharing. Advances in Cryptology CRYPTO 91,. Springer Berlin Heidelberg, pp 129-140
21. Shamir A (1979) How to share a secret. Commun ACM 11(22):612–613
22. Hasan O, Brunie L, Bertino E, Shang N (2013) A decentralized privacy preserving reputation protocol for the malicious adversarial model. Inf Forensics Secur J 8(6):1-14
23. Dolev S, Ostrovsky R (2000) Xor-trees for efficient anonymous multicast and reception. ACM Trans Inf Syst Secur 3(2):63–84
24. Goldreich O (2000) Foundations of cryptography: volume 1, basic tools. Cambridge University Press, New York
25. Naccache D, Stern J (1998) A new public key cryptosystem based on higher residues. Proceedings of the 5th, ACM Conference on Computer and Communications Security, pp 59–66
26. Goldwasser S, Micali S (2004) Probabilistic encryption. J Comput Sci Contr Syst 28:108–119
27. Okamoto T, Uchiyama S (1998) A new public-key cryptosystem as secure as factoring. EUROCRYPT 1998: 308–318
28. Benaloh J (1994) Dense probabilistic encryption. In: Proceedings of the workshop on selected areas of cryptography. Kingston, pp 120–128
29. Boneh D, Goh E-J, Nissim K (2005) Evaluating 2-DNF formulas on ciphertexts. Theory of cryptography TCC, Springer Berlin Heidelberg, pp 325–341
30. Gentry C (2009) Fully homomorphic encryption using ideal lattices. In: Proceedings of the forty-first annual ACM symposium on Theory of computing STOC. ACM, New York, NY, USA, pp 169–178
31. Beimel A, Dolev S (2003) Buses for anonymous message delivery. J Cryptology 16(1):25–39

32. Goldreich O (2004) Foundations of cryptography: volume 2, basic applications. Cambridge University Press, New York
33. Pohlig SC, Hellman ME, (1978) An improved algorithm for computing logarithms in GF(p) and its cryptographic significance. IEEE Trans. Inf. Theory 24(1):106–110
34. El Gamal T (1985) A public key cryptosystem and a signature scheme based on discrete logarithms. In: Proceedings of CRYPTO 84 on Advances in cryptology. Springer-Verlag New York, Inc, New York, NY, USA, pp 10–18
35. Boneh D (1998) The decision Diffie-Hellman problem. In: Proceedings of Algorithmic Number Theory, Third International Symposium, ANTS-III., pp 48–63
36. Benaloh J (1987) Verifiable secret-ballot elections. Ph.D. thesis. Yale University

doi:10.1186/2196-064X-1-8
Cite this article as: Dolev *et al.*: **Efficient private multi-party computations of trust in the presence of curious and malicious users.** *Journal of Trust Management* 2014 **1**:8.